

## **REMARKS**

### **Status of the application**

This paper is responsive to the Final Office Action mailed on February 27, 2007 ("Final Office Action"). Claims 1–80 are pending in this application. Claim 1–80 stand rejected. Claims 10, 15, 55, 61 and 71 are amended herein. Applicants respectfully submit the following remarks in support of patentability.

### **Claim amendments**

Claims 10 and 15 are amended herein to correct typographical errors (extraneous word "the" and repetition of the word "for," respectively). Since the nature of the errors was apparent, there is no change in the scope of either claim.

Claim 55 is amended herein to import a limitation of claim 61, and thereby simplify the discussion. Claim 61 is correspondingly amended to remove the same limitation. A typographical error (extraneous word "carrier") is also corrected in claim 55.

Claim 71 is also amended herein to simplify the discussion.

All the claim amendments are supported by the specification, and no new matter has been added.

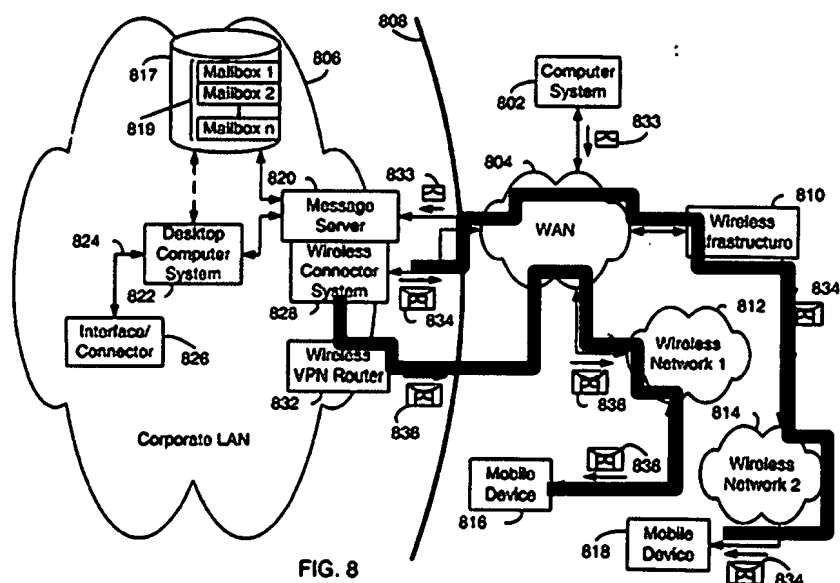
### **Claim rejections under 35 U.S.C. § 102**

Claims 1–4, 9–18 and 22–80 stand rejected under 35 U.S.C. § 102(e) over US 2004/0205248 to Little et al. ("Little"). Applicants respectfully request withdrawal of the rejections for at least the following reasons.

Preliminarily, we note that some of the claims now pending were previously rejected over a different reference, US 2004/0171369, also to Little et al. Since the Final Office Action does not make any mention of US 2004/0171369, the following discussion will be limited to US 2004/0205248. In any event Applicants believe that the same arguments apply to both references.

It will be helpful for the following discussion to summarize the teachings of Little. Little generally relates to communication systems including mobile communication

devices. A representative communication system is shown in FIG. 8 of Little, replicated below (annotations added for clarity):



Little's system includes at least two paths between the corporate LAN 806 and mobile devices 816 and 818, as indicated by the two thick lines overlaid on the figure. Little at ¶ 0069. A first path, indicated by numeral 836, passes through wireless connector system 828, wireless VPN router 832, wide area network (WAN) 804 and wireless network 812 to reach mobile device 816. Little at ¶ 0072. The VPN router establishes a virtual private network (VPN) connection through a wireless network by relying on an addressing scheme such as IPv6, which provides a dedicated IP address to each mobile device. *Id.* A second path, indicated by numeral 834, travels through wireless connector system 828, WAN 804, wireless infrastructure 810, and wireless network 814, to reach mobile device 818. Little at ¶ 0073.

Little indicates that the wireless connector system 828 may employ either a "pull" technique, in which data is transmitted in response to a request from the mobile device, or a "push" technique, in which such request is generally not necessary. Little at ¶ 0067. The wireless connector system may also employ "some combination of both techniques." *Id.* Little does not, however, teach "pushing" data in the manner claimed herein, therefore it

fails to anticipate the claimed subject matter. For clarity of presentation, each of the independent claims is separately discussed below.

**Claim 1** recites the limitation that “*the relay arrangement is arranged behind the firewall arrangement and is configured to push the data from behind the firewall arrangement to the at least one wireless device such that the data is not transmitted until the at least one wireless device can receive the data*” (emphasis added). For the reasons that follow, Applicants submit that Little fails to teach this limitation. In the Final Office Action the teachings of Little were described as follows:

[Little discloses that] the relay arrangement is arranged behind the firewall arrangement and is configured to push the data from behind the firewall arrangement to the at least one wireless device such that the data is not transmitted until the at least one wireless device can receive the data (i.e., The wireless connector system 828 may instead employ a “pull” technique, in which items stored in a mailbox 819 are sent to a mobile device 816, 818 responsive to a request or access operation made using the mobile device or some combination of both techniques) (page 8, par. 67–68 — wherein sending the message responsive to a request or access operation naturally takes place when the mobile device is on and available to pick up the message).

Final Office Action at 4. In evaluating the relevance of Little, it is important to distinguish between “push” and “pull” techniques. A “pull” technique requires the mobile device to initiate data transmission. On the other hand, a “push” technique places the initiative on the wireless connector system. Only one side in a transaction can be the initiator—either the mobile device requests transmission, or the wireless connector system initiates transmission. Little’s casual statement means at most that a single system may *alternate* between the two techniques according to the user’s convenience. However one cannot “push” an item while it is also being “pulled” from the other side, and vice versa one cannot “pull” an item while it is also being “pushed.”

Little clearly explains how its version of the “push” technique operates:

The wireless connector system 828 sends or mirrors, via a wireless network 812 or 814, certain user-selected data items or parts of data items from the corporate LAN 806 to the user’s mobile device 816 or 818, preferably upon detecting that one or more triggering events has occurred. A triggering event includes, but is not limited to, one or more of the following: screen

saver activation at a user's networked computer system 822, disconnection of the user's mobile device 816 or 818 from the interface 826, or receipt of a command sent from a mobile device 816 or 818 to the host system to start sending one or more messages stored at the host system.

Little at ¶ 0079. Clearly, neither the activation of a screen saver nor the disconnection from an interface is related to whether a mobile device can or cannot receive data items. For example, a user can disconnect a mobile device from the interface 826 (thus activating the trigger) but the mobile device could be turned off, or the user could travel outside the range of a wireless network. Therefore the only passage in this text relevant to claim 1 is "receipt of a command sent from a mobile device 816 or 818 to the host system to start sending one or more messages stored at the host system." Little at ¶ 0079. But this trigger clearly contemplates a "pull" system—not the "push" approach expressly recited in claim 1. Accordingly, Little fails to teach a "push" technique wherein "the data is not transmitted until the at least one wireless device can receive the data."

With respect to the path 836 (traveling through the wireless VPN router 832), Little fails to meet the limitations of claim 1 for a second, independent reason. Claim 1 expressly requires that "the relay arrangement . . . is configured to *push* the data" (emphasis added). Applicants submit that the wireless VPN router discussed in Little does not implement a "push" technique as intended herein. Little mentions the use of an "off-the-shelf VPN component" which "would . . . make it possible to push information to a mobile device . . . at any time." Little at ¶ 0072. However, the VPN feature allows items to be "pushed" only after the VPN has been established. The establishment of the VPN requires the active involvement of the mobile device, which cannot receive the data without first authenticating itself and its user, exchanging encryption keys with the wireless VPN router, etc. In other words, the mobile device must initiate the VPN (i.e., "pull" the connection) before any item can be pushed. The present invention allows a true "push" operation without these additional steps (and their associated overhead):

In the present invention shown in FIG. 2, the data to be transmitted is not sent beyond the exclusive security and domain of the enterprise until the wireless carrier's network 240, 250, 260 is "up" and the intended recipient's handheld 270a, 270b. 270c is "on", is within a service coverage area, and is logged onto the wireless carrier's network 240, 250, 260.

Specification at ¶ 0025. Accordingly, Little fails to teach or suggest the express limitation of claim 1 that “the relay arrangement . . . is configured to push the data.”

Finally, with respect to path 834 (traveling through wireless infrastructure 810), Little fails to teach another limitation of claim 1, namely, that “the relay arrangement is arranged behind the firewall arrangement.” In order to understand this point, it is necessary to clarify some of the functions that the “relay arrangement” performs in the context of the present invention. Little states that the use of an IPv6-based wireless VPN router “would not require . . . wireless infrastructure 90 [i.e., 810] to be used.” Little at ¶ 30. This clearly requires that the wireless infrastructure 810 perform the function of mediating between networks 804 and 814, including routing and switching data between the two networks. In other words, Little’s wireless infrastructure 810 operates as a “traffic cop” with respect to communications between the WAN 804 and the wireless network 814. The specification of the present application illustrates some of the functions that the relay arrangement 220 may perform in certain embodiments of the invention:

The relay arrangement 220 handles the routing and switching of data between the server arrangement 210 and the wireless carrier networks 240, 250 or 260. The relay arrangement 220 also executes the back-and-forth conversions between a data packet protocol according to the present invention and various protocols associated with each wireless carrier network, e.g., Mobitex’s MPAK.

Specification at ¶ 0024. Other examples of wireless protocols include GPRS, 1xRTT, and iDEN. Specification at ¶ 0004. Little provides similar examples of wireless protocols including both Mobitex and GPRS. Little at ¶ 0027. So while the wireless infrastructure of Little also performs some of the functions of a “relay arrangement” as claimed herein, it nonetheless fails to meet the limitations of claim 1 since it is located outside the firewall 808 and not behind it.

**Claim 10** recites the limitation of “the data being pushed from the relay arrangement from behind the firewall arrangement to the at least one wireless device such that the data is not transmitted until the at least one wireless device can receive the data.” Applicants submit that claim 10 is allowable for at least the same reasons as claim 1.

**Claim 14** recites the limitation that “the means for pushing is configured to push the data such that the data is not transmitted until the at least one wireless device can receive the data.” Applicants submit that claim 14 is allowable for at least the same reasons as claim 1.

**Claim 15** recites the limitation of “the relay arrangement . . . being configured to push the data from behind a firewall arrangement within the controlled network to the at least one wireless device such that the data is not transmitted until the at least one wireless device can receive the data.” Applicants submit that claim 26 is allowable for at least the same reasons as claim 1.

**Claim 24** recites the limitation that “the first arrangement is configured to push the data from behind the firewall arrangement to the at least one wireless device such that the data *is not stored outside the firewall arrangement* while enroute to the wireless carrier network” (emphasis added). Applicants submit that Little fails to teach or fairly suggest this limitation. As discussed above, Little teaches sending data to a mobile device whenever a “triggering event” is detected. It follows that Little’s system must provide for storage external to the firewall to store data while waiting for the wireless network or the mobile device to become operational. For example, as discussed in reference to claim 1, the wireless infrastructure 810 of Little stores data items outside the firewall 808 until a mobile device 818 is ready to receive them.

It is also stated in the Final Office Action that “the push technique effectively extends the company firewall 808 to include the mobile device requesting to access its messages stored on the message server 820 inside the firewall 808.” Final Office Action at 6–7. But Little makes clear that the “extension” is only a metaphor and does not imply a physical extension of the firewall: “This push technique uses a wireless friendly encoding, compression and encryption technique to deliver all information to a mobile device, thus *effectively* extending the company firewall 808 to include the mobile devices 816, 818.” Little at ¶ 0068 (emphasis added). Even assuming, for the sake of argument, that the “extension” metaphor were to be taken literally, then every component of Little’s system would be located “inside” a firewall. In that case Little would fail to meet another express

limitation of claim 24, namely that “the first arrangement is configured to push the data *from behind the firewall arrangement* to the at least one wireless device.”

**Claim 26** recites the limitation that “the relay arrangement is configured to push the data from behind the firewall arrangement to the at least one wireless device such that the data is not stored outside of the firewall arrangement while enroute to the wireless carrier network.” Applicants submit that claim 26 is allowable for at least the same reasons as claim 24.

**Claim 55**, as amended, recites the limitation that “the relay arrangement is situated behind the firewall arrangement and is configured to push the data to the at least one wireless device such that the data is not stored outside of the firewall arrangement while enroute to the wireless network.” Applicants submit that claim 26 is allowable for at least the same reasons as claim 24.

**Claim 71**, as amended, recites the limitation that “the data is not pushed beyond an arrangement to secure the data until at least one wireless device that receives data from over the wireless carrier network can receive the data.” Applicants submit that claim 26 is allowable for at least the same reasons as claim 1.

In view of the foregoing remarks, Applicants respectfully submit that all independent claims pending in this application are allowable over Little, and that dependent claims 2–4, 9, 11–13, 16–18, 22–23, 25, 27–54, 56–70 and 72–80 are also allowable for at least the same reasons.

#### **Claim rejections under 35 U.S.C. § 103**

Claims 5–8 and 19–21 were rejected under 35 U.S.C. § 103(a) over Little in view of US 6,779,039 to Bommareddy et al. (“Bommareddy”). Claims 5–8 and 19 depend from claim 1; claim 20 depends from claim 10; claim 21 depends from claim 14. Applicants submit that claims 5–8 and 19–21 are allowable for at least the same reasons as their parent claims 1, 10 and 14, and respectfully request withdrawal of the rejections.

**Conclusions**

In view of the foregoing remarks, Applicants respectfully request reconsideration, withdrawal of all grounds of rejection, and allowance of all pending claims in due course. The Examiner is invited to contact Applicants' undersigned representative by telephone at the number listed below to discuss any outstanding issues.

Respectfully submitted,

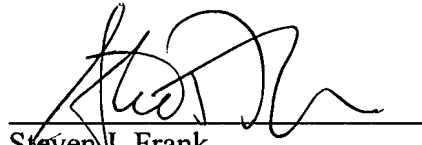
Date: May 29, 2007

Reg. No. 42,545

Customer No. 051414

Tel. No.: (617) 570-1607

Fax No.: (617) 523-1231

A handwritten signature in black ink, appearing to read "Steven J. Frank", is written over a horizontal line.

Steven J. Frank

Attorney for Applicants

Goodwin Procter LLP

Exchange Place

Boston, Massachusetts 02109